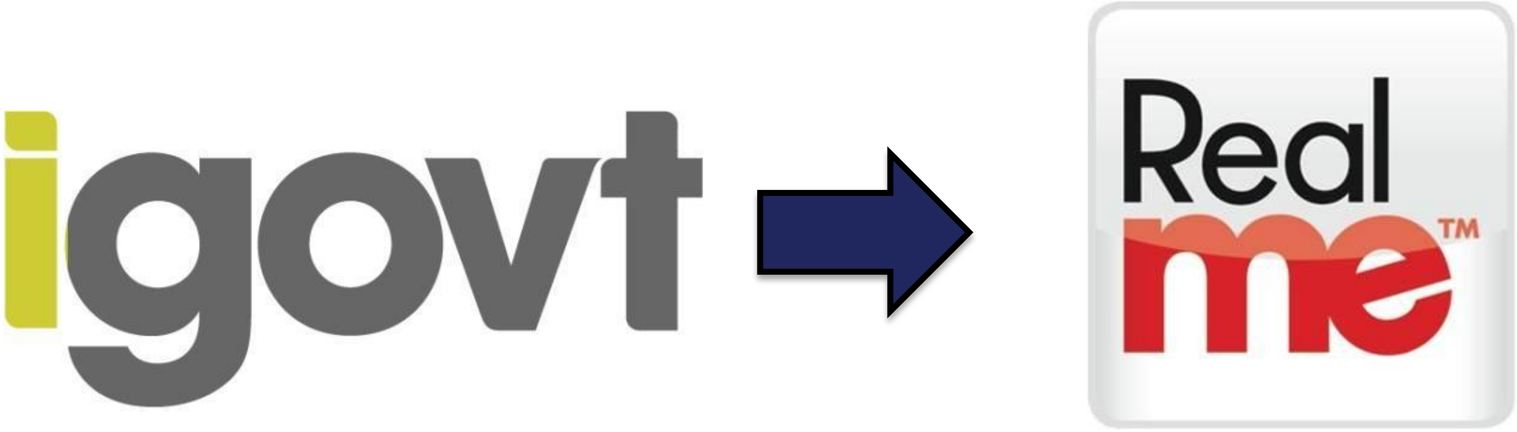
New Zealand Report Card: ‘Still in the leading bunch – more to do’
Personal analysis & observations



Government
(Internal Affairs
Dept)

NZ Post
(an SOE)

http://realme.govt.nz

Background: New Zealand's culture, policy and legislation

- Privacy legislation (EU-like) e.g. citizen controls use of/ release of data
- No national ID or ID card, no exchange of biometrics
- Low national security or illegal immigration drivers
- No Inter-agency data matching excl. few exceptions
- Citizen opt-in: Not compelled to use online services
- Agency opt-in: Not compelled to deliver via online
- Low risk, low budget approach (population: 4m)

Policy principles that are reflected eslewhere..

NZ Govt policy principles (2002) for authenticating people

- Security
- Acceptability
- Protection of privacy
- All-of-government approach
- Fit for purpose
- Opt-in

US NSTIC's guiding principles (2011)

- Secure & Resilient
- Easy to use
- Privacy enhancing
- Interoperable
- Cost effective
- Voluntary

Back in 2005 we set out to address 3 issues

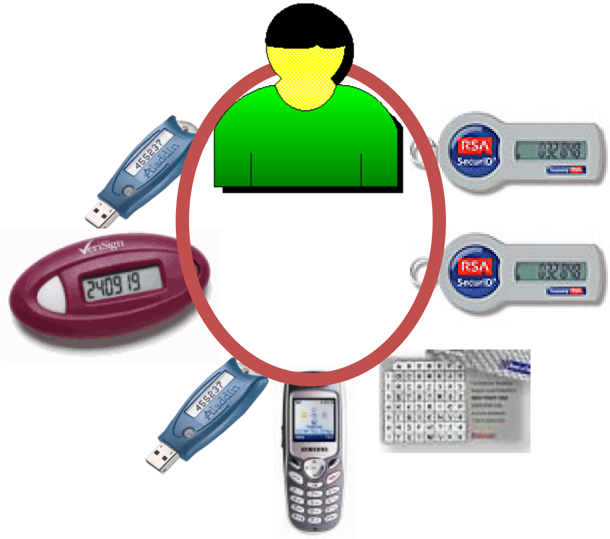
The First Issue

"On the Internet, nobody knows you're a dog."

© Internet Dog. Peter Steiner's cartoon, as published in The New Yorker

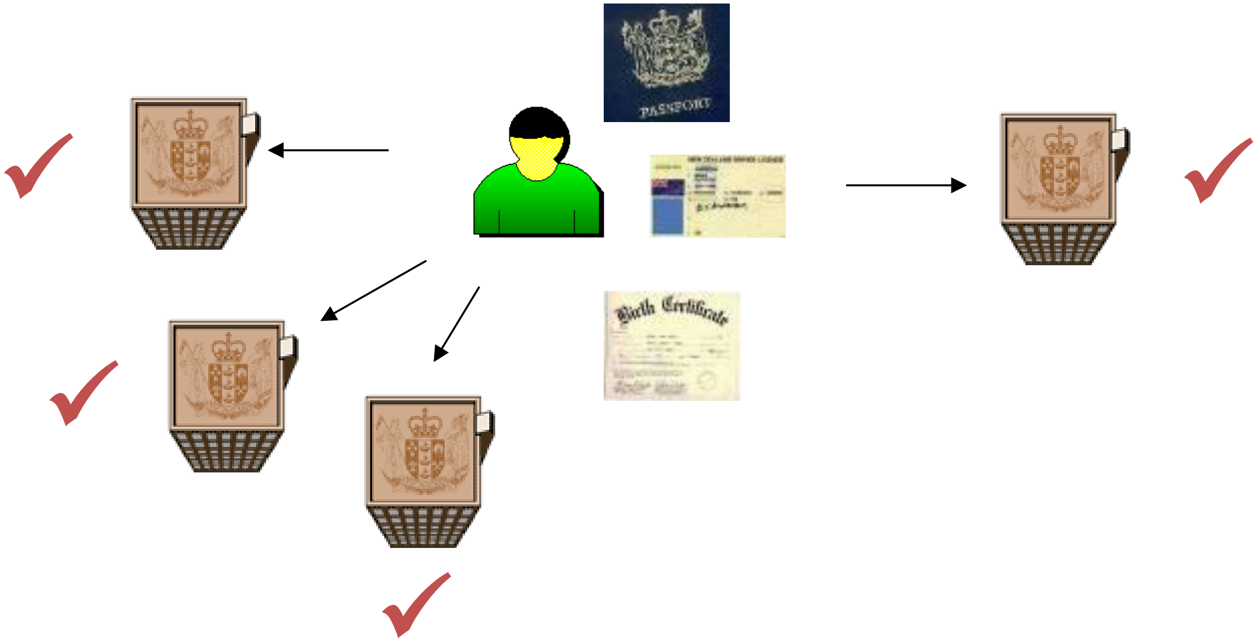
The Second Issue

- Keeping track of username and password for each online service was bad enough.
- We knew it would become worse when online services moved to two-factor authentication: “Necklace of tokens.”



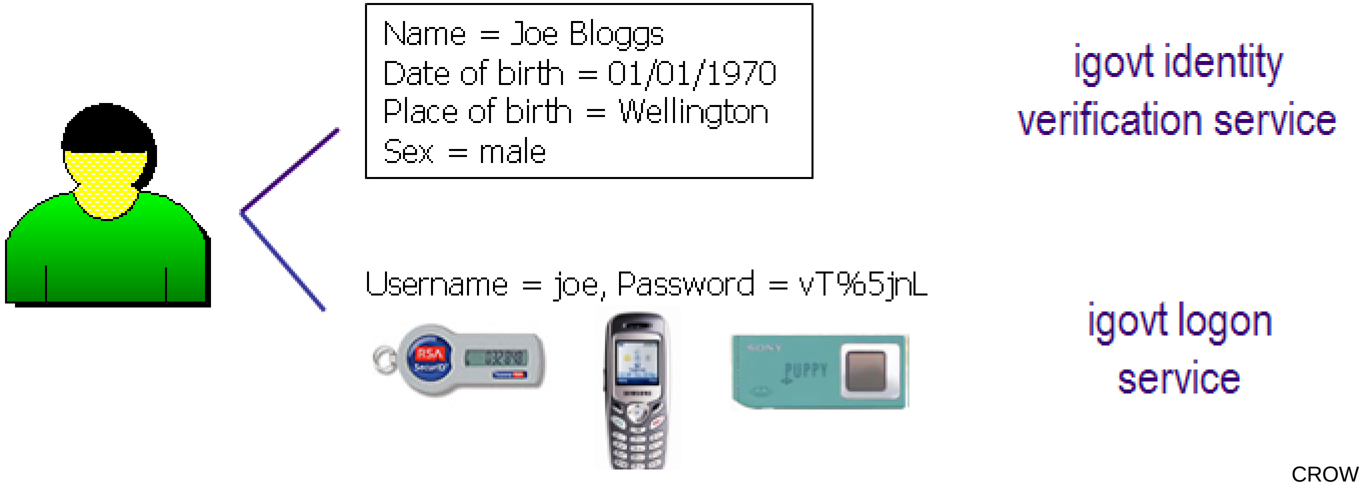
And The Third Issue

- People have to use documents to establish their identity with each government agency individually



Our approach to online authentication

- Two foundation services – both centralised but separate – identity and logon management
- Separate who a person is (identity) - from logon management functions - from what they do (activity)
- Decentralise authorisation and privilege management out to the edge



Name = Joe Bloggs
Date of birth = 01/01/1970
Place of birth = Wellington
Sex = male

igovt identity verification service

Username = joe, Password = vT%5jnL

igovt logon service

So we built 2 separate things:

- igovt pseudonymous logon service

- igovt Identity (attribute) Verification Service (IVS) that releases identity info or pseudo hashes has explicitly directed by the identity owner

Architecture for logon Authentication – 2006/7

- pseudonymous logon management (the FLT) carries no PI, designed in privacy and security with functions separated
- Take off the bottom row and the last column: what do you see?

	Credential	Credential Serial Number	Federated Logon Tag	Personal Identity information
Credential/Key Provider	✓	✓		
Government Logon Service		✓	✓	
Service Agency			✓	✓
Service User	✓			✓

‘OMB M 04 04 – like’ Identity proofing – maybe extendable to organisations, software, devices - online

EOI objective	Low EOI Confidence Level	Moderate EOI Confidence Level	High EOI Confidence Level
A – Identity exists (i.e. to determine that the identity is not fictitious)	1 document	1-2 documents (including at least one with photograph, if possible)	1-2 documents (including at least one with photograph, if possible) **or** Verification against 1-2 source records held by issuing agency
B – Identity is a ‘living identity’	(No specific process)	(No specific process)	Verification against the death register ***or*** Business processes for Objective C
C – Presenter ‘links’ to identity	(No specific process)	Verification by trusted referee **or** In-person verification	Verification by trusted referee ***or*** In-person verification **or** Biometric recognition where the agency has authorised access to a database containing the individual’s biometric information **and** Interview (in cases where suspicion is raised over individual’s identity)
D – Presenter is sole claimant of identity	Check against agency records	Check against agency records	Check against agency records
E – Presenter uses identity (i.e. use in the community)	At least 1 document/ record	At least 1 document/ record **or** Business processes for Objective C	At least 2 document/records **or** Business processes for Objective C

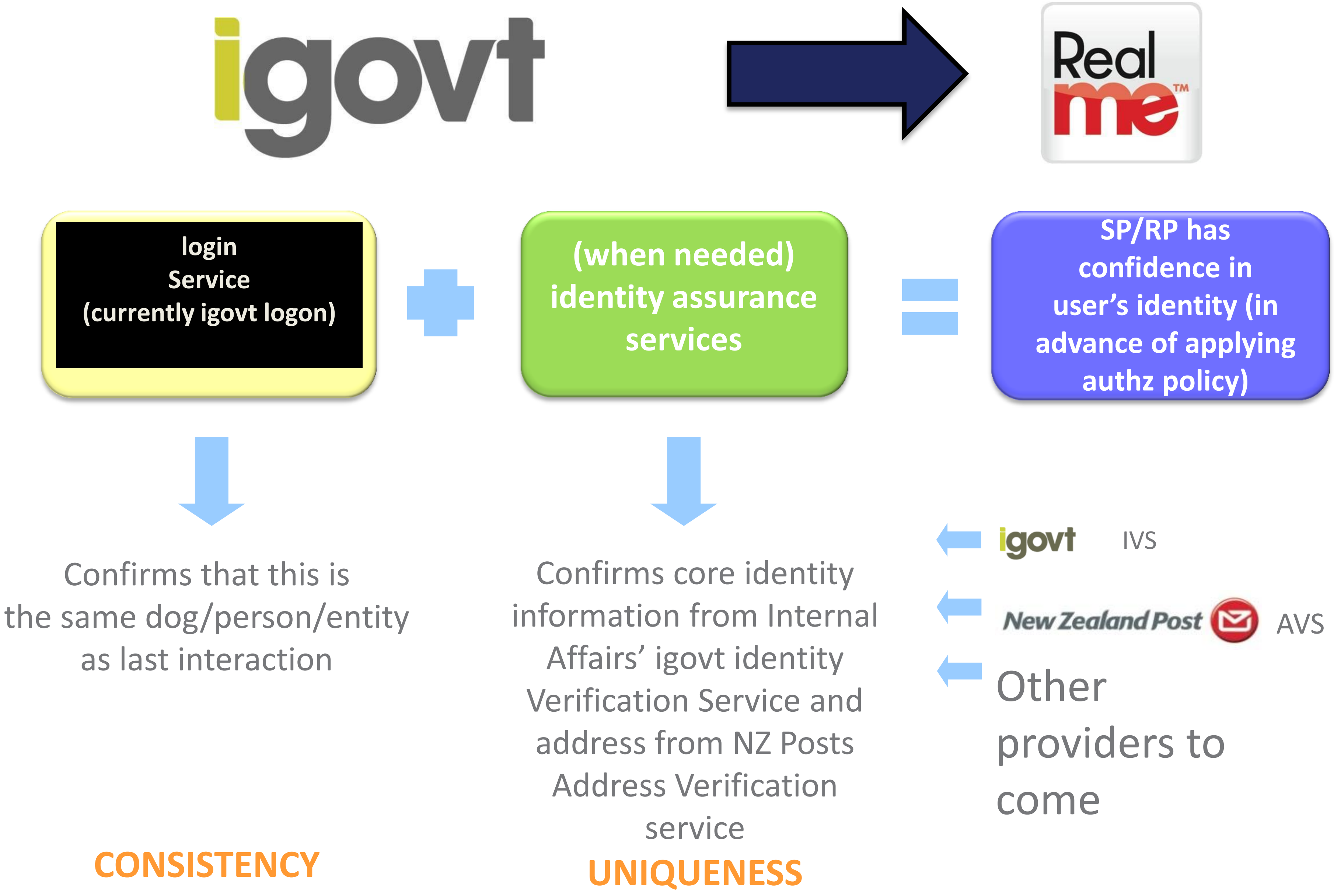
..and mapped to NZ's 'NIST 800-63- like' Authn Credential Strength Standard .. looks dated now..

Determine Service Risk Category	**Apply applicable EOI Confidence levels**	**Apply applicable Authentication keys**
Nil or negligible	None	No specific recommendation.
Low	- EOI genuine and identity used in community. - EOI accepted on 'face value'.	One-factor key: -Password conforming to the *Password Standard* **e.g. igovt password.**
Moderate	- EOI genuine and identity used in community. - Individual confirmed as genuine claimant of the identity. - EOI accepted on 'face value'.	Two-factor key that is at least: - One-time password system + password **e.g. igovt password and igovt code.** .- One-time password device + per-session activation with a password or a biometric. - Software token + per-session activation with a password or a biometric.
High	- EOI genuine and identity used in community. - Individual confirmed as genuine claimant of the identity. - EOI verified by third party.	Two-factor key that is at least: - Hardware token + per-session activation with a password or biometric.

In 2010/11 the government wanted a partner to leverage what it had built…
enter ..

New Zealand Post

about the time the US NSTIC was being drafted



igovt → RealMe

login
Service
(currently igovt logon)

+

(when needed) identity assurance services

=

SP/RP has confidence in user's identity (in advance of applying authz policy)

Confirms that this is the same dog/person/entity as last interaction

CONSISTENCY

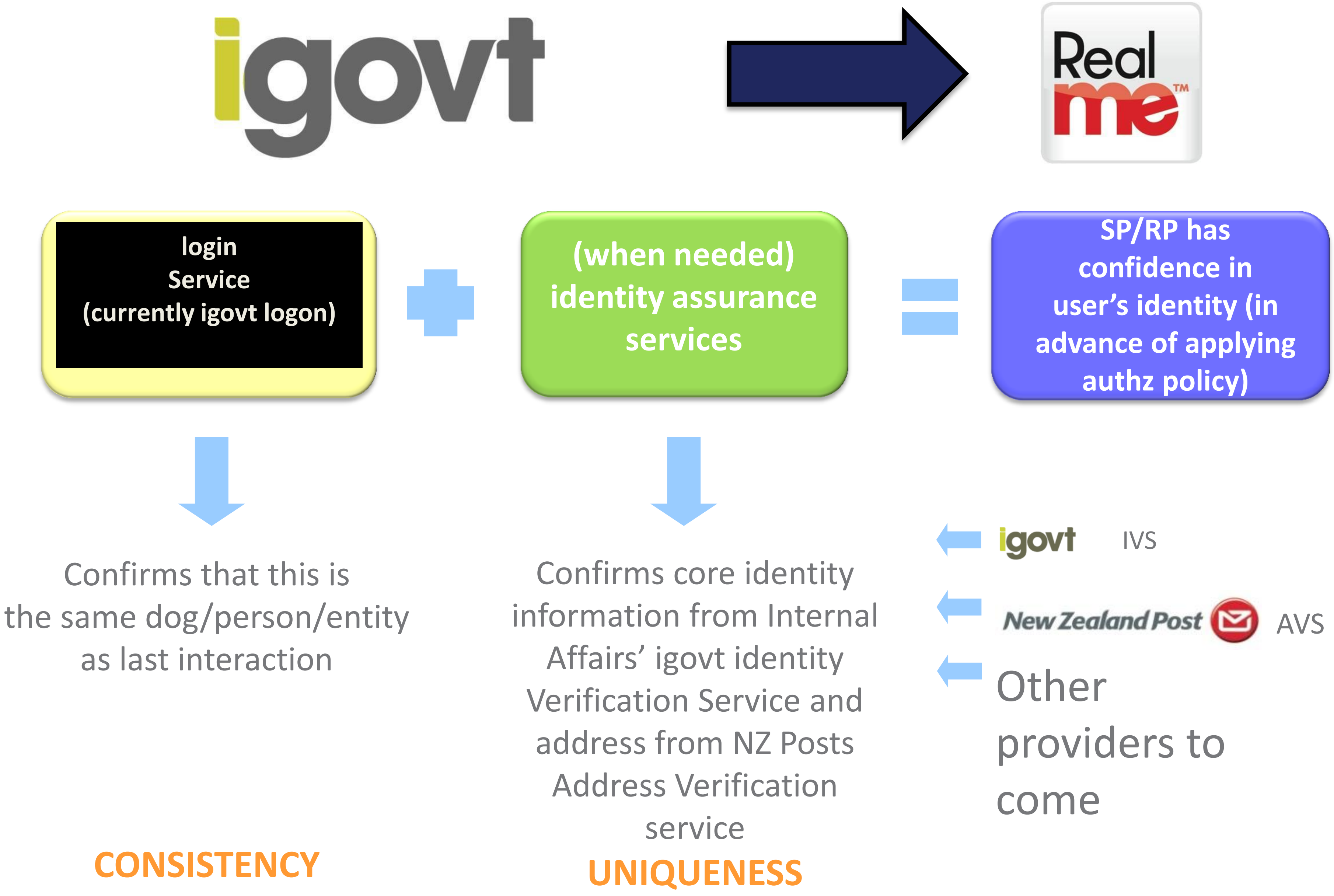
Confirms core identity information from Internal Affairs' igovt identity Verification Service and address from NZ Posts Address Verification service

UNIQUENESS

igovt IVS

New Zealand Post AVS

Other providers to come



igovt → RealMe

login
Service
(currently igovt logon)

+

(when needed)
identity assurance
services

=

SP/RP has
confidence in
user's identity (in
advance of applying
authz policy)

Confirms that this is
the same dog/person/entity
as last interaction

CONSISTENCY

Confirms core identity
information from Internal
Affairs' igovt identity
Verification Service and
address from NZ Posts
Address Verification
service

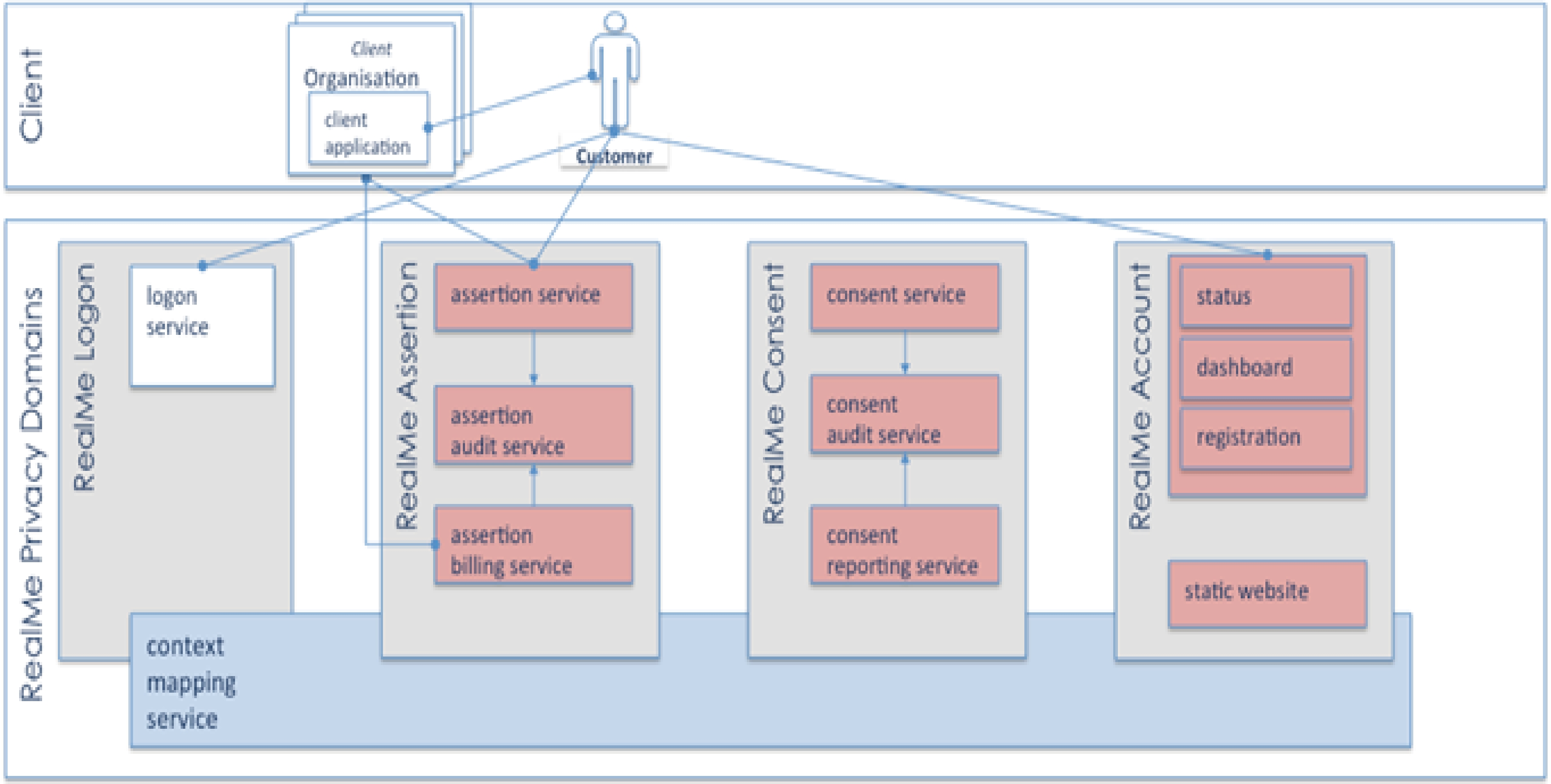
UNIQUENESS

igovt IVS

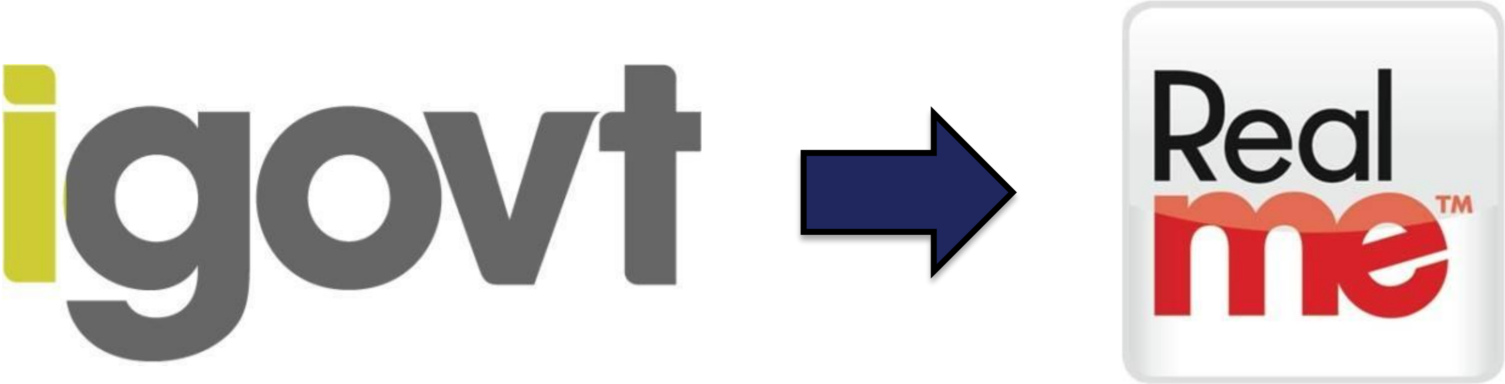
New Zealand Post AVS

Other
providers to
come

The igovt + Real me design introduces a portal and new loosely coupled services to accelerate federation with new partners, adoption of cloud services and emergence of personal cloud. The service suite, which is user accessible via SAML browser based front channel becomes: logon, assertion, consent, and the user's account dashboard.



..it’s built but will they come? ..



Government (Internal
Affairs Dept)

NZ Post (an
SOE)

Statistics pre- RealMe launch	(July 2013)
Total logons	6M
Total logon citizen ‘accounts’ Total igovtIDs created	1.5m (30% of population) 0.37m
Govt agencies connected	14/43 services (40% central agencies) doing 14.8m transactions to date

‘Still in the leading bunch – more to do’ ..personal observations.. Do you agree?

..the good

- NZ Post
- Early policy baselines 2002 and 2009, & ‘Better Govt’ policy 2012
- Supporting legislation
- Future-proofed privacy & SOA architecture patterns
- PR ‘wins’, such as online passport renewal
- Some signs of private sector engagement
- We’re up and going!

..improvement areas

- NZ Post
- Macro-economic/digital economy policy ‘lumpy’
- Governance with expert support
- ‘iGovt Logon only’ policy drives password resets
- Newer lighter protocols - OAuth, OpenID, JSON
- Mobile Authn/optimisation
- Organisation and device identity
- User centric/personal data notions
- Most of all – culture, mindset and attitude